United States Court of Appeals for the Sixth Circuit

Information Technology Security Officer

Vacancy Announcement No. 18-05

ABOUT THE COURT

The federal Judiciary seeks talented and motivated individuals to help in its mission of ensuring equal justice under law. The federal Judiciary offers work/life balance, competitive benefits, and teams with dedicated professionals. The United States Court of Appeals for the Sixth Circuit is one of 12 regional federal courts. Circuit courts hear appeals from the district (trial) courts located within their circuit, as well as appeals from decisions of federal administrative agencies. Headquartered in Cincinnati, the Court serves Kentucky, Michigan, Ohio, and Tennessee. For more information about the federal court system, please visit: www.uscourts.gov and www.ca6.uscourts.gov.

POSITION INFORMATION

Location	Cincinnati, Ohio	**Tour of Duty**	Full-Time
Opening Date	March 22, 2018	**Salary**	CL 28 ($69,884 – $99,109) *Salary commensurate with qualifications in accordance with U.S. Court Guidelines*
Closing Date	To ensure consideration, applications must be received by **April 20, 2018**. The position will remain open until filled.		

POSITION OVERVIEW

The IT Security Officer performs professional work related to the operation and management of IT security policy, planning, development, implementation, training, and support for the Sixth Circuit. The incumbent provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives within the court. The incumbent ensures the confidentiality, integrity, and availability of systems, networks, and data. The incumbent is responsible for implementing local security policies, processes, and technologies that are consistent with the national Information Security program as well as for collaborating with other judiciary stakeholders, such as the Administrative Office and other court IT personnel, to identify and collectively advance security initiatives both within and beyond court unit boundaries. Occasional travel within and outside of the Sixth Circuit is required. This position reports to the Assistant Circuit Executive for Information Technology. Refer to the complete Position Description attached to this announcement.

QUALIFICATIONS

Required: At least two years of professional IT security experience, a strong understanding of IT security best practices, and demonstrated ability to analyze, design, and implement security policies and procedures. Knowledge and expertise in network management and security, IT networks, network traffic, computer hardware and software, and data communications. Knowledge of applicable programming languages, such as Visual Basic, Java, PHP, and SQL. Ability to identify and analyze security risks and to implement resolutions. Knowledge of anti-malware and endpoint security controls. Knowledge of IPSec and the ability to use it to protect data, voice, and video traffic. Skill in designing security architecture roadmaps and documenting architecture decisions. Completion of a master's degree or two years of graduate study in computer science, or related field, may be substituted for two years professional IT experience. For those already employed in the federal system, at least one year of experience at or equivalent to CL-27.

Preferred: Bachelor's degree from an accredited university or college, preferably in computer science or related field. CISSP, CISM, or equivalent certification is strongly desired.

BENEFITS

Employees of the U.S. Courts are not classified under the civil service; however, they are entitled to the same benefits as other federal employees. The benefits include: health, dental, vision, life, and long term care insurance; annual and sick leave; paid holidays; retirement; and the judiciary's supplemental benefits. Visit www.uscourts.gov/careers for additional information regarding benefits with the federal Judiciary.

CONDITIONS OF EMPLOYMENT

Positions with the United States Courts are considered "at will" and are not subject to the employment regulations of competitive service. Appointment to position is provisional pending suitability determination by the court based on results of a background investigation and credit check. Employees are subject to the *Judicial Code of Conduct for Judicial Employees*. Employees are required to use Electronic Fund Transfer for payroll direct deposit. Visit http://www.uscourts.gov/careers for citizenship requirements. The Court of Appeals is an Equal Opportunity Employer.

APPLICATION PROCEDURE

Submit a cover letter emphasizing experience relevant to the position and detailed resume to the Human Resources Manager at: ca06-humanresources@ca6.uscourts.gov.

Updated 04/02/2018

Job Title	IT Security Officer	CL - 28
Occupational Group*	Professional Administrative	

Job Summary

The IT Security Officer performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for the Sixth Circuit. The incumbent provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives within the court. The incumbent ensures the confidentiality, integrity, and availability of systems, networks, and data across the system development life cycle (SDLC), and creates, promotes, and adheres to standardized, repeatable processes for the delivery of security services. The IT Security Officer pro-actively engages all users in security awareness and training activities to promote the appropriate use of best security practices within the court. The incumbent is responsible for implementing local security policies, processes, and technologies that are consistent with the national Information Security program as well as for collaborating with other judiciary stakeholders, such as the Administrative Office and other court IT personnel, to identify and collectively advance security initiatives both within and beyond court boundaries.

Representative Duties

- Review, evaluate, and make recommendations on the court's technology security program, including automation, telecommunications, and other technology utilized by the court. Promote and support security services available throughout the court.
- Provide technical advisory services to securely design, implement, maintain, or modify information technology systems and networks that are critical to the operation and success of the court. Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate managers/personnel of the risk potential.
- Provide advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, and other senior court staff.
- Assist in the development and maintenance of local court security policies and guidance, the remediation of identified risks, and the implementation of security measures.
- Develop, analyze, and evaluate new and innovative information technology policies that will constructively transform the information security posture of the court. Make recommendations regarding best practices and implement changes in policy.
- Provide security analysis of IT activities to ensure that appropriate security measures are in place and are enforced. Conduct security risk and vulnerability assessments of planned and installed information systems to identify weaknesses, risks, and protection requirements. Utilize standard reporting templates, automated security tools, and cross-functional teams to facilitate security assessments.
- Assist with the identification, implementation, and documentation of security safeguards on information systems. Manage information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order, in a timely manner, and according to schedule. Prepare justifications for budget requests. Prepare special management reports for the court, as needed.
- Serve as a liaison with court stakeholders to integrate security into the system development lifecycle. Educate project stakeholders about security concepts, and create supporting methodologies and templates to meet security requirements and controls.
- Recommend changes to ensure information systems' reliability and to prevent and defend against unauthorized access to systems, networks, and data.
- Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the courts' information technology security services.
- Establish mechanisms to promote awareness and adoption of security best practices.

Factor 1 – Required Competencies (Knowledge, Skills, and Abilities)

Information Technology Security and Automation

- Knowledge and expertise in the theories, principles, practices and techniques of network management and security, IT networks, network traffic, computer hardware and software, and data communications. Knowledge of applicable programming languages, such as Visual Basic, Java, PHP, and SQL. Ability to analyze IT security problems and assess the practical implications of alternative solutions. Ability to identify and analyze security risks and to implement resolutions. Knowledge of anti-malware and endpoint security controls. Knowledge of IPSec and the ability to use it to protect data, voice, and video traffic. Ability to work with other court divisions within the circuit in order to collaborate on best practices. Skill in designing security architecture roadmaps and documenting architecture decisions.

Project Management

- Ability to assist in leading projects, including organization knowledge, analysis, documentation, reporting, recommending, and strategic thinking. Skill in resolving technical, administrative, and operational problems, providing recommendations to users, service providers, and senior management.
- Demonstrated ability to effectively analyze and synthesize diverse input, establish priorities, and complete multiple projects. Knowledge and understanding of the steps required in developing secure IT systems and making modifications to ensure that appropriate security measures are in place and are enforced.

Court Operations

- Knowledge and understanding of the structure and functions of the federal courts at the local court unit level, with emphasis on specific mission critical systems, in order to provide advice on projects. Skill in analyzing court IT security needs. Knowledge of local court policies and procedures regarding IT security and system accountability.

Judgment and Ethics

- Knowledge of and compliance with the *Code of Conduct for Judicial Employees* and local court confidentiality requirements. Ability to consistently exercise sound ethics and judgment in dealing with confidential matters and information.

Written and Oral Communication/Interaction

- Ability to communicate effectively (orally and in writing) to individuals and groups to provide information. Ability to interact effectively and professionally with others, providing customer service and resolving difficulties while complying with regulations, rules, and procedures. Skill in translating and documenting technical terms into non-technical language. Skill in training non-automation personnel in automation techniques and processes.

Factor 2 – Primary Job Focus and Scope

The work performed directly impacts the ability of the court to effectively perform its core functions and operational duties. The primary focus of the position is to develop and implement IT security policies, procedures, and technologies to ensure court IT systems operate optimally and without risk of security breaches. The IT Security Officer is responsible for development and implementation of effective IT security solutions to improve workflow within the courts. The incumbent provides advice and makes recommendations to court unit executives, judges, and senior staff to resolve complex security issues by assessing risk and analyzing options. The incumbent's work includes all areas of automation, telecommunications, and technology utilized by the court. The work directly impacts the efficiency and the integrity of the court and is essential to the overall mission and core functions of the circuit. The established routine work of the court is dependent on its automated systems. Proper functioning of information management systems ensures the timeliness and accuracy of actions in all segments of the court. The work of the court would be compromised or disrupted by a security breach or incident. The IT Security Officer's active participation in development and successful implementation of national level IT security initiatives substantially impacts systems throughout the judiciary.

Factor 3 – Complexity and Decision Making
The IT Security Officer evaluates and makes decisions within the context of professional standards, broad policies, and according to the goals and mission of the court. The systems and equipment impacted are varied and complex, each with its own ever-changing security vulnerabilities. Choosing among different security approaches, each with potential risks is a routine requirement. The incumbent must consider efficiency and economy in evaluating alternatives; yet, the systems must operate with little or no disruption. In the event of a security incident, the incumbent must make quick decisions and implement corrective action, often without full information. The IT Security Officer works independently, coordinates the work with other courts, and refers to the guidance from the circuit. While technical input on particular strategies may be obtained from multiple sources, such as the AO Office of Information Technology Security Office, the incumbent must rely primarily on personal technical and managerial skills and abilities.

Factor 4A – Interactions with Judiciary Contacts
The primary judiciary contacts are court unit executives, judges, IT peers, IT supervisors, chambers staff, court staff, and other IT users to provide immediate solutions to both complex and routine problems, and to provide guidance. Outside of the court, technical contacts with personnel from other courts, judicial law enforcement personnel, and the AO are made for the purpose of resolving specific problems, collaborating on system developments, leveraging judiciary-wide contracts, sharing information, and ensuring local needs are reflected in national level efforts.

Factor 4B – Interactions with External Contacts
Outside contacts are with security professionals and network management experts concerning emerging threats, new strategies, and problems with currently installed software. The incumbent contacts vendors and service representatives to plan, coordinate work, solicit advice on efforts, resolve operating problems, and introduce new IT systems or procedures. Due to the evolving nature of information security, the incumbent is also expected to establish formal and/or informal relationships with recognized security experts, such as SANS, NIST, and US CERT.

Factor 5 – Work Environment and Physical Demands
Work is performed in an office setting. Minimal travel is required. Duties require working during non-business hours. Incumbents may be required to lift moderately heavy items.

Rev. 3/22/2018